Journal of KIIT. Vol. 18, No. 7, pp. 43-50, Jul. 31, 2020. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.7.43

CBDC 간 교환을 위한 ISO/IEC 11179기반 블록체인 시스템

정 현 준*

ISO/IEC 11179-based Blockchain System for Exchange Between CBDCs

Hyunjun Jung*

요 약

CBDC(Central Bank Digital Currency)란 중앙은행에서 발행하는 디지털 화폐를 말한다. 국가들은 금융위기를 겪고 현금 없는 사회를 대비하여 CBDC를 연구하였다. 최근 전 세계는 전염병으로 인해 소비심리가 위축되고 경기 침체를 피하고자 기본소득을 지급을 고려하고 있다. 국가의 재정정책을 정교하게 운용할 방법으로 CBDC가 다시 한 번 주목받고 있다. 많은 나라는 CBDC를 연구하고 있으며 특히 중국은 발행을 적극적으로 검토 중이다. 중앙은행은 여러 나라의 CBDC가 발행되고 교환하는 상황을 고려해야 한다. 이 논문은 CBDC 간의 교환을 위한 ISO/IEC 11179 메타데이터 레지스트리 기반의 블록체인 시스템을 제안한다. 각 나라의 CBDC는 구현방식과 발행 시기가 다를 것이다. CBDC에 대한 공통된 표현을 위하여 우리는 ISO/IEC 11179 메타데이터 레지스티리 기반 표현방법과 관리하는 방법을 제안한다. 이 논문에서는 등록되어있는 CBDC 간의 거래를 기록하는 블록체인 시스템을 제안한다. 그리고 우리는 블록체인 시스템을 구현하고 동작 방법을 실험한다. 마지막으로 제안방법과 암호화폐 거래소(중앙화 방식, 탈중앙화 방식)를 비교한다.

Abstract

Central Bank Digital Currency (CBDC) is a digital currency issued by a central bank. Countries are researching the CBDC against the financial crisis and cashless society. Recently, the world considers paying basic income to avoid consumer sentiment shrinks and recession due to epidemics. CBDC is coming into the spotlight as the way to run elaborately the public finance policy of nation. The many countries are studying CBDC and especially China is positively the publication. The central bank should consider the situation in which CBDCs from different countries are issued and exchanged. This paper proposes a blockchain system based on ISO/IEC 11179 metadata registry for exchange between CBDCs. Each country's CBDC will have a different implementation and time of publication. For common expression of CBDC, we propose an ISO/IEC 11179 metadata registry-based expression and management method. In this paper, We implement the blockchain system and experiment with the operation method. And We measure the block generation time of Blockchains using the proposed method. Finally, we compare the proposed method with the cryptocurrency exchange (centralized, decentralized).

Keywords
CBDC, CBDC exchange, ISO/IEC 11179, CBDC exchange blochchain system

* 광주과학기술원 블록체인인터넷경제연구센터 연구원
- ORCID: https://orcid.org/0000-0002-6717-1395

· Received: Apr. 13, 2020, Revised: Jun. 11, 2020, Accepted: Jun. 14, 2020
· Corresponding Author: Hyunjun Jung
Blockchain Internet Economy Research Center, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea; junghj85@gmail.com
Tel.: +82-62-715-3140, Email: junghj85@gist.ac.kr

Ⅰ. 서 론

우리는 인터넷은행 등의 등장으로 은행 업무를 오프라인보다 온라인에서 진행하는 것이 익숙하다. 온라인 네트워크에서 우리가 주고받는 것은 실제 돈이 아닌 데이터이다. 은행은 계좌별로 발생하는 거래를 거래장부에 저장한다. 은행은 거래장부의 데이터 무결성을 지키기 위하여 큰 비용을 지급한다. 은행은 거래장부의 외부공격을 막기 위하여 거래장부가 저장된 서버의 외부인터넷 연결을 차단하기도 한다. 우리는 데이터 무결성을 위해서 신뢰받는 제3의 중개자에게 의존하며 높은 비용을 지급하고 있다. 비트코인은 제3자의 신뢰 대신 암호학적 증명(Cryptographic proof)에 기반한 P2P(Peer-to-peer) 전자화폐 시스템을 제안하였다[1]. 비트코인은 블록체인 기술을 이용한 대표적인 암호화폐로 대중들에게 알려지게 되었다. 블록체인은 암호화폐를 통하여 은행이 하나의 거래장부를 지키는 방식에서 거래고객들이 모두 투명하게 거래장부를 가지고 있는 방식으로 패러다임을 전환했다. 우리는 블록체인을 통하여 모든 거래를 실시간으로 확인할 수 있으며, 위-변조되지 않았음을 서로 상호증명한다. 암호화폐에서는 은행과 같은 중개자가 필요 없으며, 중개자에게 내던 신뢰 유지비용을 거래장부를 유지하는 사람들에게 배분한다. 암호화폐는 중개자가 없는 특성을 이용하여 우리는 부의 재분배를 유도할 수 있다고 주장한다[2][3].

비트코인의 등장 이후로 수많은 암호화폐가 만들어졌다. 리플(Ripple)은 전 세계은행들 사이에서 실시간 자금 송금을 지원하기 위하여 제안되었다[4]. 리플은 국제송금의 시간과 비용을 줄이기 위하여 제안된 암호화폐이다. 리플은 세계 각지의 은행들이 기술적 한계 혹은 이해관계의 상충으로 인하여 실행되지 못하고 있는 실생활의 문제를 블록체인 기술로 접근한다. 국제송금은 SWIFT(Society for Worldwide Interbank Financial Telecommunication)를 이용하여 송금하면 수취하기까지 2~3시간 소요되며 은행마다 수수료가 상이하다. 리플은 암호화폐를 이용하여 송금 비용을 절감하고 효율적으로 처리하는 것을 목표로 한다. 이처럼 암호화폐들은 실생활에 문제를 해결하기 위하여 아이디어를 제안하고 현실의 빅 브러더에게 혁신을 요구하고 있다.

각 나라의 중앙은행은 현금 없는 사회를 대비하여 CBDC(Central Bank Digital Currency)를 연구하기 시작했다. 현금 없는 사회란 신용카드, 모바일 지급수단 등의 비현금 지급수단 이용 활성화로 현금사용이 감소한 사회를 말한다. 스웨덴, 영국, 뉴질랜드 등의 현금 없는 사회로 진입되었다고 평가되는 나라들은 공통으로 국민의 현금 접근성 약화, 취약계층의 금융 소외, 소비 활동 제약, 공적 화폐유통시스템 약화의 문제점이 발생하였다. 중앙은행은 CBDC에 대한 필요성은 확인했지만, 실제 개발과 도입까지는 일부 나라에서만 실험적으로 시행되었다. 하지만 암호화폐의 등장으로 CBDC는 다시 한 번 주목을 받게 되었다.

국제결제은행(BIS, Bank for International Settlements)은 3년 내 세계 인구의 20%가 CBDC를 접할 것이라고 예상했다[5]. 국제결제은행은 특히 신흥국이 CBDC 발행을 빠르게 추진하고 있고 선진국은 신중한 태도를 보인다고 밝혔다. 각 나라는 CBDC를 도입했을 때의 영향에 대하여 대비가 필요하다.

이 논문은 CBDC 간의 거래방법에 대하여 제안한다. CBDC 간의 거래는 기존의 암호화폐 거래와는 다르게 구상되어야 한다. CBDC는 발행 주체가 명확하며 실물화폐와 1:1 교환을 보증한다. CBDC의 교환을 위해서는 발행 주체인 중앙은행 간의 식별을 위한 공조가 필요하다. 그리고 국가 간의 화폐 이동을 중앙은행이 보증하고 기록으로 남겨야 한다.

이 논문에서는 CBDC 교환을 위하여 ISO/IEC 11179 메타데이터 레지스트리(Metadata registry)기반의 블록체인 시스템을 제안한다. 이 논문에서는 CBDC의 일관성 있는 관리와 공유를 위한 메타데이터 레지스트리 기반의 CBDC 설계를 제안한다. 그리고 CBDC 간 교환을 위한 블록체인 동작 방법을 제안한다.

이 논문에서 2장은 암호화폐 교환에 관한 관련 연구를 소개한다. 3장은 ISO/IEC 11179 기반의 CBDC 관리방법과 블록체인 동작 방법을 제안하다. 4장은 제안한 CBDC 블록체인을 구현한 프로토타입을 소개한다. 5장은 암호화폐 교환방법들과 비교 평가한다. 마지막으로 6장에서는 결론을 제시한다.

II. 관련 연구

이 장에서는 암호화폐 교환에 관한 연구를 소개한다. 암호화폐를 법정화폐나 다른 암호화폐로 교환하기 위하여 거래소를 이용한다. 거래소는 서버-클라이언트 방식의 중앙화 방식 거래소와 탈중앙화 분산형 거래소(DEX, Decentralized Exchange)가 있다. 중앙화 방식의 거래소는 고객의 개인 키를 소유하여 거래하는 방식으로써 거래소에 보안을 의지한다. 탈중앙화 거래소 방식의 거래소는 P2P 방식으로 암호화폐 간의 거래를 수행한다. 그리고 탈중앙화된 분산거래소를 만들기 위해서는 아토믹 스왑(Aatomic swap) 기능을 구현해야 한다[6].

현재 많은 국가가 CBDC의 연구개발에 긍정적인 태도를 보이며 현금의 발행 비중을 줄이고 거래 편의성을 높일 수 있다고 믿는다. 국제결제은행은 CDBC가 편리성, 탄력성, 접근성, 개인정보보호, 국경 간 지불에 대한 사용 편의성을 제공해야 한다고 발표했다[7]. 영국 중앙은행은 RSCoin의 개발을 런던 대학교에 의뢰하여 연구를 진행하였으며 구체적인 CBDC 발행 계획은 없다[8]. 캐나다 중앙은행은 CBDC 기술을 이용한 실시간 총액결제와 증권청산결제 시스템을 구축하는 Jasper 프로젝트를 진행했다[9]. 싱가포르 중앙은행은 거액결제와 증권청산결제 시스템을 구축하는 Ubin 프로젝트를 진행했다[10]. 현재 연구 동향은 CBDC의 구축에 집중되어 있다.

Han[11]는 CBDC의 아키텍처와 비즈니스 프로세스 그리고 해외결제 방법에 대한 프레임워크를 제안하였다. 프레임워크는 CBDC 간의 해외결제를 위하여 블록체인 네트워크를 운영한다. 거래자들은 ID를 이용하여 거래를 작성하고 은행 또는 제3의 운영자에게 제출한다. 거래 요청을 받은 은행 또는 제3의 운영자는 AML 작업을 수행하고 거래가 준수되는지 보증한다. 그리고 블록체인은 스마트 계약을 이용하여 CBDC 간의 거래 트랜잭션을 실행한다.

III. 제안방법

이 장에서는 ISO/IEC 11179 기반의 국가별 CBDC를 등록하고 관리하는 방법을 제안한다. 그리고 CBDC 간의 교환을 위한 블록체인 시스템을 제안한다. 기존 연구는 각 나라의 중앙은행들이 CBDC의 구축과 운영에 관련되어 진행되었다. 그리고 CBDC 간의 거래에 관한 연구가 개념적으로 제안되었다. 이 논문은 CBDC 간의 거래를 위한 CBDC 설계 방법과 블록체인 시스템의 구현방법에 대하여 다룬다. 제안한 CBDC 설계 방법을 이용하여 각 나라의 CBDC를 일관된 형태로 표현하고 공유하고 관리할 수 있다. 제안한 블록체인 시스템은 관리되고 있는 CBDC 간에 거래를 저장하고 실행하는 방법에 대하여 제안한다.

3.1 ISO/IEC 11179 기반 CBDC 설계

ISO/IEC 11179 메타데이터 레지스트리(Information technology - Metadata Registry, MDR)는 메타데이터의 등록과 인증을 통하여 메타데이터를 유지와 관리하는 메타모델이다[12]. MDR은 데이터 요소(Data element)의 생성과 등록관리를 지원하여 시스템 간 정보를 공유한다. MDR은 데이터의 의미, 표현, 식별을 쉽게 하여 데이터의 사용자들이 쉽게 이해할 수 있게 한다. 그리고 메타데이터 수집의 일관적 모델을 제공한다.

제안방법은 CBDC를 MDR의 사상에 따라 데이터 요소로 표현하고 관리하고자 한다. 효율적인 CBDC의 교환은 보내는 사람과 받는 사람이 같은 CBDC 정보로 해석하는 것을 보장하는 환경에서 이루어진다. CBDC 정보의 공유가 가능하도록 표준화된 의미와 형태를 가진 CBDC 정보 요소가 필요하다. 각 국에서 만든 CBDC를 내부적인 거래처리는 각 CBDC 운영 측에서 보장해야 한다. 반면에 CBDC 외부적인 거래는 어떻게 주고받을지에 대한 약속이 필요하다. MDR은 데이터를 이해할 수 있고 공유할 수 있도록 만들기 위한 표준화와 등록에 관한 내용을 설명하고 있다. MDR에 의해 관리되는 데이터의 기본단위는 데이터 요소이다.

그림 1은 제안하는 ISO/IEC 11179 기반 CBDC 정보저장 방법의 개요를 보여준다. 중앙은행은 CBDC를 데이터 요소 구성에 따라 CBDC MDR에 저장한다. CBDC MDR은 블록체인에 저장되는 거래내용을 식별하기 위하여 사용된다.

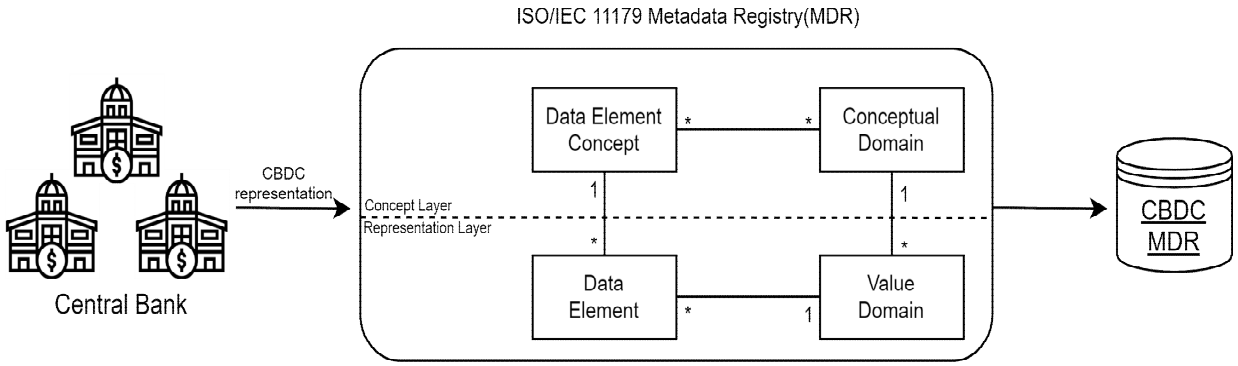

그림 1. ISO/IEC 11179 기반 CBDC 정보저장 개요
Fig. 1. Overview of ISO/IEC11179 based CBDC MDR

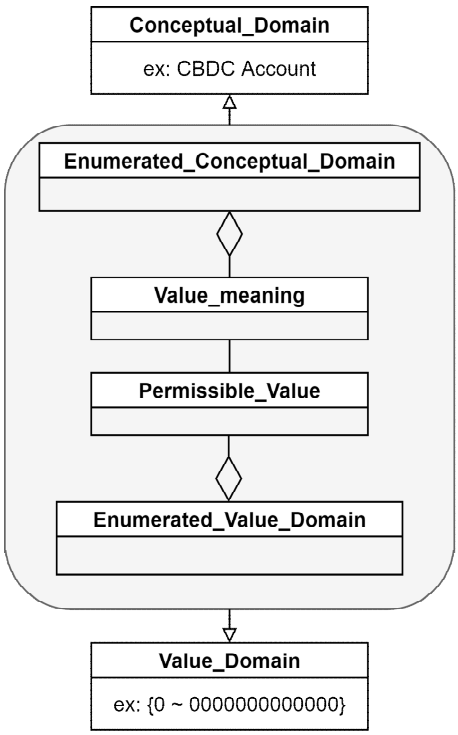

그림 2. 개념 도메인과 값 도메인 예
Fig. 2. Conceptual domain and value domain example

MDR에서 데이터 요소는 개념 층(Concept layer)과 표현 층(Representation layer)으로 분류한다. 개념 층은 데이터 요소 개념(Data element concept)과 개념 도메인(Conceptual domain)으로 데이터가 속한 개념, 도메인 등을 나타낸다. 표현 층에서는 데이터 요소와 값 도메인(Value domain)으로 데이터값의 형식, 측정 단위 등을 나타낸다. MDR을 이용하면 데이터의 개념적인 구분과 데이터값에 대한 표현 정보를 얻을 수 있다. 그림 2는 개념 도메인과 값 도메인의 예를 보여준다.

MDR의 데이터 값에 대한 표현은 개념 도메인과 값 도메인을 이용하여 표현한다. 데이터는 서술형과 열거형으로 구분하여 표현할 수 있다. 서술형은 Described 개념 도메인과 Described 값 도메인으로 서술되어있는 데이터의 의미를 표현한다. 열거형은 Enumerated 개념 도메인, Value meaning, Permissible value, Enumerated 값 도메인으로 열거할 수 있는 데이터의 의미를 표현한다. CBDC는 열거형을 이용하여 정해진 데이터 표현할 수 있다. 예를 들어 비트코인에서 BTC(비트코인), Satoshi(사토시) 등의 단위와 표현범위를 정할 수 있다. 이더리움은 ETHER, WEI 등의 단위와 표현범위를 정할 수 있다.

3.2 CBDC 교환을 위한 블록체인

이 장에서는 CBDC 간의 교환을 위한 MDR 기반의 블록체인 시스템을 설명한다. 제안하는 MDR 기반 블록체인은 CBDC 간의 거래에 관한 내용을 저장한다. 제안하는 블록체인을 이용하면 각 나라의 CBDC의 구현형태와 상관없이 교환할 수 있다. 거래에 참여한 중앙은행은 CBDC 거래에 관련된 계약 트랜잭션을 작성한다. 그리고 중앙은행은 작성한 트랜잭션이 블록에 생성할 때 CBDC의 발행과 소각을 실행한다. 이를 통하여 신속한 CBDC의 거래와 보안성을 보장할 수 있다.

그림 3은 MDR 기반의 블록체인 모델의 개요도이다. 제안하는 블록체인 시스템은 MDR에 등록한 중앙은행 그룹이 노드로 참여하여 운영한다. 제안하는 블록체인 시스템은 블록의 Transaction에 CBDC 간 거래내용을 담는다.

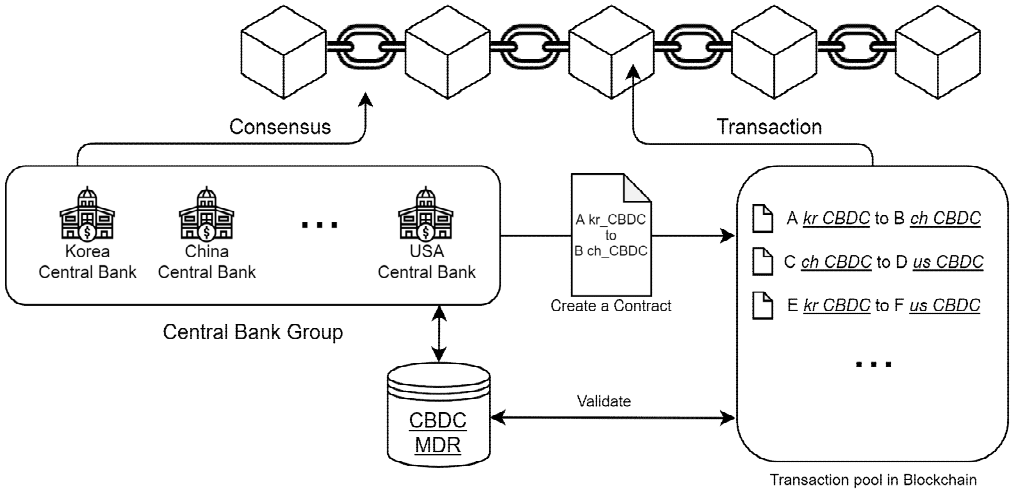

그림 3. MDR 기반 블록체인 모델 개요도
Fig. 3. MDR-based CBDC blockchain model

그리고 블록체인의 합의(Consensus)는 블록체인 그룹 노드에 의해 결정된다. Transaction 내용에는 보내려는 금액과 CBDC 주소 (ex: A kr_CBDC)와 받는 금액과 CBDC 주소(ex: B ch_CBDC)로 구성할 수 있다. CBDC MDR은 Transaction에 저장된 계약의 유효성 검증을 도와준다.

Ⅳ. 실 험

이 장에서는 3장에서 제안한 CBDC 교환을 위하여 블록체인 시스템 검증 실험을 한다. 제안하는 블록체인 시스템은 CBDC 간의 거래내용을 저장한다. 블록체인 시스템에 저장되는 트랜잭션은 MDR에 관리되고 있는 CBDC 간의 데이터이다. 이를 블록체인 시스템에 저장하기 위해서는 임의의 데이터를 저장해야 한다. 실험에서는 Bitcoin을 이용하여 우리가 만든 임의의 CBDC 데이터를 저장하는 방법에 대하여 검증한다.

블록체인에 저장기능을 이더리움은 Smart contract를 사용할 수 있고, 비트코인은 OP_RETURN 스크립트를 이용하여 수행할 수 있다. 이 실험에서는 비트코인을 하드포크하여 실험을 진행하였다. 비트코인은 블록에 임의의 데이터를 넣을 수 있게 트랜잭션 내에 OP_RETURN 스크립트를 제공한다. OP_RETURN은 Bitcoin Core 0.9버전부터 지원하는 기능으로 한 번에 최대 80 bytes를 기록할 수 있다[13]. 이 실험에서는 OP_RETURN 스크립트에 CBDC 거래내용을 저장한다. 블록체인에 문자 “100 krcbdc, 200 chcbdc”는 Hex “313030206b72636264632c323030206363626463”으로 변환되어 OP_RETURN에 저장된다.

그림 4는 Hex 값으로 변환된 OP_RETURN 값을 저장한 raw 트랜잭션을 만드는 과정이다. 트랜잭션을 만들기 위해서는 txid를 선택하고 트랜잭션을 작성해야 한다. 트랜잭션은 검색한 txid, “data”에 저장하려는 Hex 값을 넣어 생성한다.

```
jun@ubuntu:~/bitcoin_ECC$ bitcoin-cli createrawtransaction
'[{"txid":"a9be24c77cb20ddc519cf965847dff4ba1a8bc39252ba88d1c2135ffe630bc08","vout":0}]'
'{"data":"313030206b72636264632c323030206363626463",
"3AtMh9Sq6yHPFAxnPXNZp3foMLckDxHToo":49.9995}'
result:
020000000108bc30e6ff35211c8da82b2539bca8a14bff7d8465f99c51dc0db27cc724bea90000000000ffffff
fff020000000000000000176a15313030206b72636264632c323030206363626463626463b02e052a0100000017a9
1464de35c0d2cad5282eb82ca3fe38368a45d45b348700000000

jun@ubuntu:~/bitcoin_ECC$ bitcoin-cli signrawtransactionwithkey
"020000000108bc30e6ff35211c8da82b2539bca8a14bff7d8465f99c51dc0db27cc724bea90000000000ffff
ffff020000000000000000176a15313030206b72636264632c323030206363626463626463b02e052a0100000017a
91464de35c0d2cad5282eb82ca3fe38368a45d45b348700000000"
'["Kzk1pFT3Utbnh49NsU63UKqposxwMejhiuFghzh39nvkgjyeNR5M"]'
result:
{
  "hex":
"020000000010108bc30e6ff35211c8da82b2539bca8a14bff7d8465f99c51dc0db27cc724bea90000000017
16001491a2236d1444d976f5a2d141befdec4793fefe8bffffffff020000000000000000176a15313030206b7
2636264632c323030206368636264632463b02e052a0100000017a91464de35c0d2cad5282eb82ca3fe38368a45d4
5b348702473044022056580d7608cc33f863e07c8cffb796af0daede7697fa6787ca10f9d8a82c9020022059e
8151045acb6df34f89533f19f5e6ae6af5f270b3cc42f0ca0eab54fe28f8501210367a02f9237c6d43ca425a6
b7c3bd79b30ef9722212c84b945b27f6e7d69d07df00000000",
  "complete": true
}

jun@ubuntu:~/bitcoin_ECC$ bitcoin-cli sendrawtransaction
020000000010108bc30e6ff35211c8da82b2539bca8a14bff7d8465f99c51dc0db27cc724bea900000000171
6001491a2236d1444d976f5a2d141befdec4793fefe8bffffffff020000000000000000176a15313030206b72
636264632c323030206368636264632463b02e052a0100000017a91464de35c0d2cad5282eb82ca3fe38368a45d45
b348702473044022056580d7608cc33f863e07c8cffb796af0daede7697fa6787ca10f9d8a82c9020022059e8
151045acb6df34f89533f19f5e6ae6af5f270b3cc42f0ca0eab54fe28f8501210367a02f9237c6d43ca425a6b
7c3bd79b30ef9722212c84b945b27f6e7d69d07df00000000
result:
43c73cdd07feac6b144f5bb265dfe5c9e8b49755f3d7d4cb6a26a009c23e4ec8
```

그림 4. 트랜잭션 생성과 송출
Fig. 4. Create and send raw transaction

그림 5는 블록의 정보를 확인하여 트랜잭션 저장소에 송신한 트랜잭션이 삽입되었는지 보여준다. 생성한 블록을 getblock 명령어를 이용하여 확인한 결과를 보면, 송신한 트랜잭션 해시가 기록되어있음을 확인할 수 있다. 그림 6은 삽입된 트랜잭션 내용을 해독한 것이다. 중간에 OP_RETURN 값에 원하는 데이터가 제대로 들어갔음을 확인할 수 있다.


```
jun@ubuntu:~/bitcoin_ECC$ bitcoin-cli getblock
53f0d55317ae6b07c1c30f08d1df894256fdb2b221e80dbe48189fe7964c8180
{
  "hash": "53f0d55317ae6b07c1c30f08d1df894256fdb2b221e80dbe48189fe7964c8180",
  "confirmations": 1,
  "strippedsize": 352,
  "size": 497,
  "weight": 1553,
  "height": 11,
  "version": 536870912,
  "versionHex": "20000000",
  "merkleroot": "c935f13c7a7d5a2a7108de07ce9b588c1f878af723fe79e32c9f2d0ac58afe7e",
  "tx": [
    "4522ff707df70006068cfb84c66c90a3b8b4c889b9c91faf5ef3c1ef1e781c79",
    "43c73cdd07feac6b144f5bb265dfe5c9e8b49755f3d7d4cb6a26a009c23e4ec8"
  ],
  "time": 1591853494,
  "mediantime": 1591852713,
  "nonce": 11,
  "bits": "00000001",
  "difficulty": 4.523059468369196e+74,
  "chainwork": "00000000000000000000000000000000000000000000000000000000000005f2e0",
  "nTx": 2,
  "previousblockhash": "eef88b7a9748d83d6dfd30f7eafa66b3a8ae6ab2777c0ca5841d5e0462280f93"
}
```


그림 5. 트랜잭션을 블록에 삽입
Fig. 5. Insert transaction to block


```
jun@ubuntu:~/bitcoin_ECC$ bitcoin-cli decoderawtransaction
020000000010108bc30e6ff35211c8da82b2539bca8a14bff7d8465f99c51dc0db27cc724bea900000001716001491a2236d1444d976f5a2d141befdec4793
fefe8bffffffff0200000000000000000176a1531303020bb72636264632c32303020636863626463b02e052a0100000017a91464de35c0d2cad5282eb82ca3fe
38368a45d45b3487024730440220565804d7608cc33f863e07c8cffb796af0daede7697fa6787ca10f9d8a82c9020022059e8151045acb6df34f89533f19f5e6a
e6af5f270b3cc42f0ca0eab54fe28f850121036 7a02f9237c6d43ca425a6b7c3bd79b30ef9722212c84b945b27f6e7d69d07df00000000
result:
{
  "txid": "43c73cdd07feac6b144f5bb265dfe5c9e8b49755f3d7d4cb6a26a009c23e4ec8",
  "hash": "3ee8ea27563b481d0977f3dfaf9bb19f9cb490e84cb0b1a8b2025e8ecb882cf8",
  "version": 2,
  "size": 247,
  "vsize": 166,
  "weight": 661,
  "locktime": 0,
  "vin": [
    {
      "txid": "a9be24c77cb20ddc519cf965847dff4ba1a8bc39252ba88d1c2135ffe630bc08",
      "vout": 0,
      "scriptSig": {
        "asm": "001491a2236d1444d976f5a2d141befdec4793fefe8b",
        "hex": "16001491a2236d1444d976f5a2d141befdec4793fefe8b"
      },
      "txinwitness": [

"304402056580d7608cc33f863e07c8cffb796af0daede7697fa6787ca10f9d8a82c9020022059e8151045acb6df34f89533f19f5e6ae6af5f270b3cc42f0ca
0eab54fe28f8501",
        "0367a02f9237c6d43ca425a6b7c3bd79b30ef9722212c84b945b27f6e7d69d07df"
      ],
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "OP_RETURN 313030206b72636264632c32303020636863626463",
        "hex": "6a1531303020bb72636264632c32303020636863626463",
        "type": "nulldata"
      }
    },
    {
      "value": 49.99950000,
      "n": 1,
      "scriptPubKey": {
        "asm": "OP_HASH160 64de35c0d2cad5282eb82ca3fe38368a45d45b34 OP_EQUAL",
        "hex": "a91464de35c0d2cad5282eb82ca3fe38368a45d45b3487",
        "reqSigs": 1,
        "type": "scripthash",
        "addresses": [
          "3AtMh9Sq6yHPFAxnPXNZp3foMLckDxHToo"
        ]
      }
    }
  ]
}
```


그림 6. 트랜잭션 내용 (OP_RETURN)
Fig. 6. Decode raw transaction (OP_RETURN)

V. 평 가

이 장에서는 제안방법과 암호화폐 교환방법을 비교 평가한다. 제안방법에 대한 평가를 위해서는 CBDC 간의 교환방법과 비교평가가 필요하다. 하지만 현재 CBDC 간의 거래에 관한 연구는 추상적인 레벨에서 제안되어 있으며 비교가 부적절하다. 이 논문은 CBDC 간의 거래를 암호화폐 교환의 한 부분으로 구분하여 비교하였다.

암호화폐 교환방법은 중앙화 거래소 방식과 탈중앙 분산형 거래소 방식으로 구분한다.

제안방법과 블록체인 기술적용 여부, 거래당사자의 개인 키 대여 여부, 거래 자원의 양(유동성), 거래의 책임 보증자, 거래대상 암호화폐, 암호화폐 정보 관리를 비교 평가한다. 표 1은 제안방법과 관련 연구 간의 비교평가를 보여준다.

표 1. 관련 연구와 비교평가
Table 1. Comparison of proposed methods and related works

Feature	Proposed method	Centralization exchange	Decentralizaed exchange
Technical use of blockchain	Yes	No	Yes
Private key rental	No	Yes	No
Amount of fluidity	Low	High	Low
Transaction liability	Central Banks	Exchange	Unknown
Transaction target cryptocurrency	CBDC	ALL cryptocurrency	Same hash function cryptocurrency
Cryptocurrency information management	Yes (open)	Yes (close)	No

블록체인 기술적용 여부는 제안방법과 탈중앙 거래소는 블록체인을 이용하여 거래를 저장한다. 중앙화 거래소는 블록체인 대신 중앙화된 저장소를 사용한다. 블록체인 기술의 사용 여부는 거래를 중재자 없이 진행할 수 있는지를 판단할 수 있다. 블록체인을 적용한 시스템은 거래내용이 투명하게 공개하고 기술적으로 신뢰를 보장받지만, 중앙화 거래소는 거래내용을 거래소가 독점하며 거래소에 신뢰를 의존하다.

개인 키 제공 여부는 제안방법과 탈중앙 거래소는 받지 않는다. 중앙화 거래소는 개인 키를 받는다. 개인 키 제공 여부는 보안성과 밀접한 관계가 있다. 중앙화 거래소는 비밀키를 받아 거래소를 운영한다. 중앙화 거래소에 많은 금액이 모이기 때문에 해킹의 위협에 노출된다. 실제로 암호화폐의 해킹 사건은 블록체인 해킹보다 암호화폐 거래소에 대한 해킹 사건이 자주 발생하였다.

유동성의 양은 중앙화 거래소가 많으며 제안방법과 탈중앙화 거래소는 적다. 유동성의 양이 적으면 원하는 시간과 원하는 가격에 거래되기 어렵다. 하지만 제안방법은 중앙은행들의 합의에 따라 수행하기 때문에 원하는 시간에 거래할 수 있다.

암호화폐에 대한 거래 책임은 다음과 같다. 제안방법은 중앙은행, 중앙화 거래소는 거래소, 탈중앙화 거래소는 불분명하다. 제안방법은 중앙은행 그룹간의 거래이기 때문에 책임소재가 명확하다. 중앙화 거래소는 거래에 대한 책임을 지고 있으며 문제가 생길 때 법적 소송 대상이 된다. 탈중앙화 거래소는 기술적으로 거래의 신뢰성을 보증하지만, 문제가 생기면 책임소재가 불분명할 수 있다.

거래대상 코인은 다음과 같다. 제안방법은 CDBC, 탈중앙화 거래소는 같은 해시 함수인 암호화폐, 중앙화 거래소는 모든 암호화폐를 다룰 수 있다. 탈중앙화 거래소는 아토믹 스왑의 조건인 같은 해시 함수일 때 가능하다. 예를 들어 ERC-20 계열, 비트코인 하드포크 계열 등이 이에 해당한다.

암호화폐 정보 관리는 제안방법과 중앙화 방법은 가능하다. 탈중앙화 거래소는 초기에 정해진 암호화폐만 거래할 수 있다. 제안방법은 MDR 기반으로 중앙은행그룹이 공개적으로 관리한다. 중앙화 거래소는 거래소에서 허용하는 암호화폐를 추가 관리할 수 있다.

Ⅵ. 결 론

이 논문은 CBDC의 연구에 관한 관심이 높아지고 있는 현 상황에서 CBDC 간에 교환을 위한 시스템을 제안한다. CBDC는 하나의 공통된 방식으로 구현되고 공급되기는 힘들 것이다. 하지만 공통으로 CBDC는 중앙은행 혹은 상응하는 기관에서 관리하고 책임질 것이다. 이 공통점에 착안하여 이 논문은 ISO/IEC 메타데이터 레지스트리 기반의 블록체인 시스템을 제안한다. 이 시스템에서 교환을 원하는 중앙은행들은 자신의 CBDC를 메타데이터 레지스트리 요소에 따라 서술하여 저장한다. CBDC마다 구현방법은 다르지만, 공통된 표현으로 CBDC를 표현하고 공유할 수 있다. 그리고 중앙은행은 지속해서 CBDC에 대하여 관리할 수 있다. 이 논문에서 제안하는 메타데이터 레지스트리 기반의 CBDC 블록체인 모델은 중앙은행이 등록해놓은 CBDC 간의 거래내역을 블록에 저장한다. 중앙은행들의 발행(Mint)과 소각(Burn)에 대한 권한을 이용하여 거래내용에 대하여 계약(Smart contract)을 한다. 그리고 블록에 트랜잭션이 저장되기 전에 각 CBDC를 발행 및 소각을 진행한다. 이를 통하여 CBDC 간의 거래를 완료하고 거래내용은 블록체인에 남게 된다.

제안한 방법을 보여주기 위하여 비트코인을 하드포크하여 CBDC 블록체인 모델 적용을 실험하였다. 실험은 MDR을 이용하여 생성된 거래내용을 블록에 넣는 과정을 진행하였다. 마지막으로 제안방법과 중앙화 거래소, 탈중앙화 거래소와 비교하였다. 비교결과 보안성과 거래대상에 대한 관리 측면에서 유리한 점이 있다고 보인다.

이 논문은 각국의 중앙은행에서 CBDC에 대한 필요성이 확대되고 있는 이때, 만들어진 CBDC 간에 어떻게 공유할지에 대하여 다루었다. 추후연구에서 각 중앙은행의 CBDC가 좀 더 대중화된다면 기존의 환전 시스템과 정량적으로 비교하고자 한다.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Nov. 2009. https://bitcoin.org/bitcoin.pdf, [accessed: Mar. 14. 2020]

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain", Business & Information Systems Engineering, Vol. 58, pp. 183-187, Mar. 2017.

[3] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to

sustainable supply chain management", International Journal of Production Research, Vol. 57, No. 7, pp. 2117-2135, Oct. 2018.

[4] Ripple, https://ripple. com/ [accessed: Mar. 14. 2020]

[5] C. Boar, H. Holden, and A. Wadsworth, "Impending arrival - a sequel to the survey on central bank digital currency", Bank for international settlements, Jan. 2020. https://www.bis.org/publ/bppdf/bispap107.htm, [accessed: Mar. 14. 2020]

[6] H. Maurice, "Atomic cross-chain swaps", In: Proceedings of the 2018 ACM symposium on principles of distributed computing, Egham United Kingdom, pp. 245-254, Jul. 2018.

[7] R. Auer and R. Boehme, "The technology of retail central bank digital currency", BIS Quarterly Review, 16pages, Mar. 2020.

[8] G. Danezis, S. Meiklejohn, "Centrally banked cryptocurrencies", 2015, https://arxiv.org/abs/1505.06895, [accessed: Mar. 14. 2020]

[9] R. Garratt, "CAD-coin versus Fedcoin", 2016. https://www.r3cev.com/s/Cad-coin-versus-Fedcoin-rg, [accessed: Mar. 14. 2020]

[10] S. Mohanty and N. N. Sin, "The future is here Project Ubin: SGD on Distributed Ledger", Monetary Authority of Singapore(MAS), Feb. 2017.

[11] X. Han, Y. Yuan, and F.Y. Wang, "A Blockchain-based Framework for Central Bank Digital Currency", 2019 IEEE International Conference on Service Operations and Logistics and Informatics (SOLI), Zhengzhou, China, pp. 263-268, Nov. 2019.

[12] ISO, "ISO/IEC 11179-1:2015 Information technology — Metadata registries (MDR) Part 1: Frame work", 2015.

[13] Bitcoin Wiki, "OP_RETURN" https://en.bitcoin.it/wiki/OP_RETURN, [accessed: Mar. 14. 2020]

저자소개

정 현 준 (Hyunjun Jung)

2008년 : 삼육대학교 컴퓨터과학과(학사)
2010년 : 숭실대학교 컴퓨터학과(공학석사)
2017년 : 고려대학교 컴퓨터·전파통신공학과(공학박사)
2017년 8월 ~ 현재 : 광주과학기술원 블록체인인터넷경제연구센터
관심분야 : 블록체인, 데이터 사이언스, 센서 네트워크, 사물인터